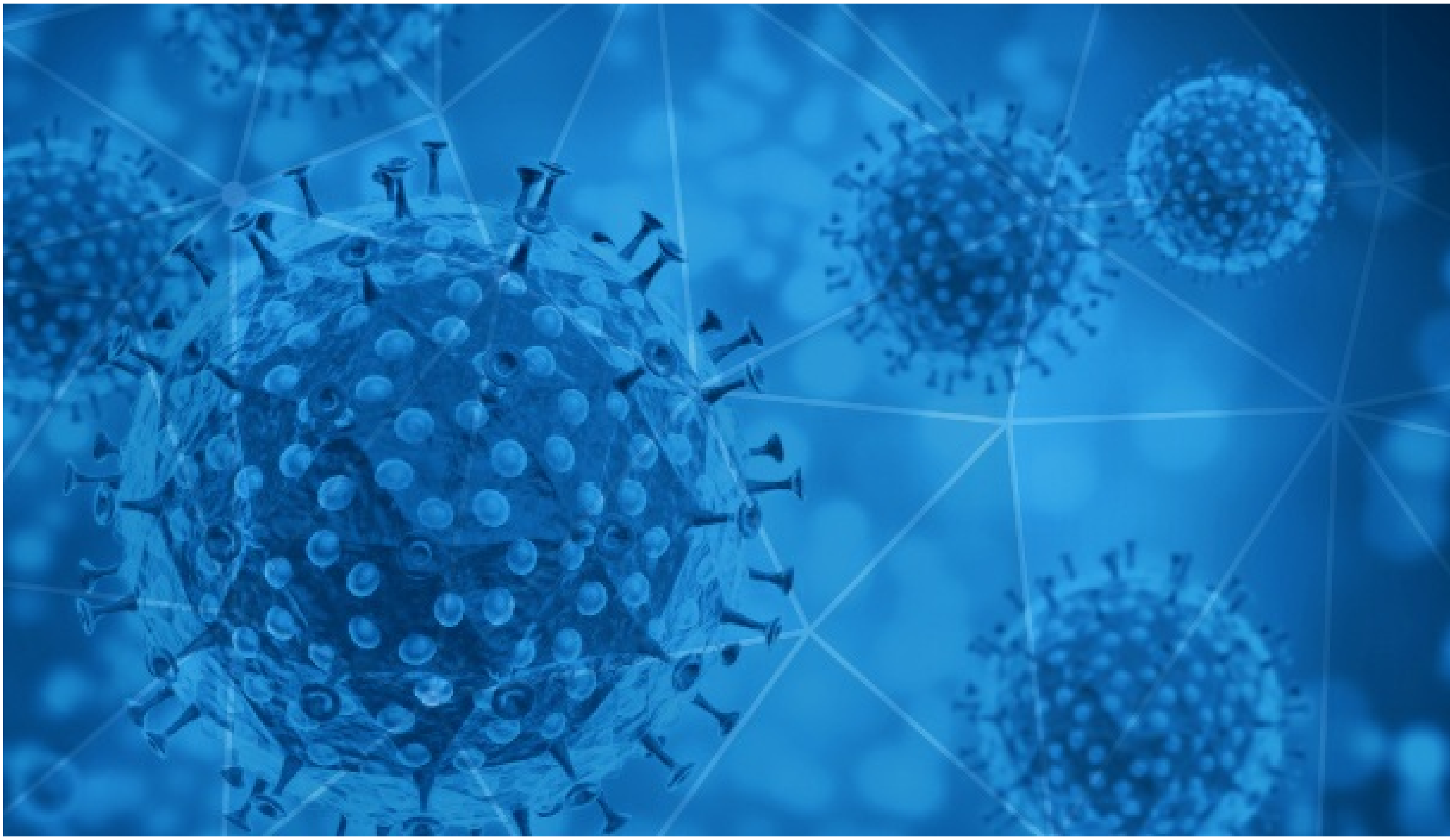
RiskIQ i3:

Finished Intelligence Indicator of Compromise (IOC) COVID-19 Report

2021-01-20



Methodology

The information provided in this report is limited to open source and publicly available data discovered through standard, commonly known browsing techniques and keyword searches. To provide efficient results, RiskIQ may use websites that require payment in exchange for aggregation of data that is otherwise publicly available without payment and could be obtained by anyone accessing the correct sites or engaging the correct third parties to obtain the information. Information presented in this report is cross-checked against multiple sources for full verification; however, some assessments and conclusions are based on incomplete information and represent the RiskIQ analyst's judgment based on patterns and data available.

Disclaimer

The information provided in this report is "AS-IS" and Customer acknowledges and agrees that RiskIQ makes no representation or warranty, express or implied, as to the accuracy or completeness of the information. The customer agrees that RiskIQ shall not have any liability resulting from their use of this information.

Notice

As of 05/15/2020 RiskIQ changed the format and frequency of the COVID-19 Daily Update. Each Friday, RiskIQ will compile the week's major stories in the Notable Events, Facts and Figures at a Glance, Stay-At-Home/Shelter-In-Place Orders, and Governmental Guidance sections of the report.

The Digital Exploitation data will continue to be delivered daily with the COVID-19 Email Spam Statistics, COVID-19 Host, Domain, and Mobile App Tracking, and COVID-themed Blacklisted Domains included.

RiskIQ has established a microsite for COVID-19 coverage, located at https://www.riskiq.com/covid19-cybersecurity/.

Thank you for your continued readership!

Daily Blacklisted Hosts Feed

RiskIQ is making a blacklisted host feed from its COVID-themed scanning available to the public. Blacklisted hosts listed in the feed have been observed serving scammy/fraudulent content, phish, malware, or malicious code. This data is delivered "AS-IS".

https://covid-public-domains.s3-us-west-1.amazonaws.com/covid19_blacklist.html

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 2021-01-19 to 2021-01-20. During this period, RiskIQ analyzed 28,405 spam emails containing either “*corona*” or “*COVID*” in the subject line. There were 4,592 unique subject lines observed during the reporting period. The spam emails originated from 2,340 unique sending email domains and 4,180 unique SMTP IP Addresses. Analysts identified 1 emails which sent an executable file for Windows machines.

Top-25 Subjects

The Corona Letter: A compromised immune system?	4158
Man Lived Inside Airport for 3 Months over COVID fear +Mitch McConnell says Trump PROVOKED MAGA RIOT	1013
Test rápidos Covid 9,95 €, Generador de ozono 39,95 €. purifica 25 m². Evita contagios	842
COVID Notice: Hospital-Grade Disinfectant made available to public here	689
Covid-19 Global Relief Fund	675
Are you Alive? (Covid -19 Security Alert)	492
COVID19 Winter Surge Is Here- Stock Up ON KN95 Certified Mask And Get 50%!O(MISSING)ff Today	488
Health Officials Urge To Wear KN95 Certified Mask To Help Curve COVID19- Take 50%!O(MISSING)ff Today	475
Arma tu Kit contra el Covid-19	413
COVID-19 PANDEMIC COMPENSATION FUND	336
Defeat Coronavirus, Thermographic Camera	327
Contactless infrared body temperature thermometer defeat Coronavirus	326
Puricador y Sanitizador de Aire, Estirilización contra Coronavirus	316
Covid-19 relief funds	309
Re: Defeat Coronavirus, non contact fever alarm device	305
COVID-19 Memorial: A national moment of unity and remembrance	304
Thermographic Automation Camera defeat Coronavirus	303
Re: Digital signage solution for Covid-19	279
HERZLICHEN GLÜCKWUNSCH, CASH COVID-19 PALLIATIVEN AUS MEINEN LOTTERIEGEWINNEN	259
Direct Client Req:: Need SAP ABAP Developer, Tallahassee, FL, Long Term, REMOTE UNTIL COVID!	250
Re: covid-19 epidemic prevention supplies, such as kinds of face masks, nitrile glove...etc.	232
Gran Venta Outlet - Productos Covid 19	228
COVID19 LOAN FROM THE UNITED NATIONS WITH NO INTEREST RATE	226
COVID-19 DONATION FOR YOU! GET BACK TO ME NOW...	217
Stay Protected From COVID19 Using KN95 Authentic Mask- Shipping Is Waived Today	202

COVID-19 Email Spam Statistics (Continued)

Top-15 Domains Sending COVID Spam

timesofindia.com	4160
gmail.com	1496
keyable.net	1261
caribbeanfever.com	1013
kn95certified.store	965
hospiramedical.co.uk	934
amonmed.es	842
thermopenis.guru	689
fundstepnltdinfo.com	675
mailinator.cl	425

Top-15 IPs Sending COVID Spam

113.116.205.249	1261
194.116.228.152	963
195.62.32.174	689
51.79.158.32	673
85.204.116.109	670
180.235.232.196	492
5.56.22.142	427
5.56.22.141	411
193.140.109.251	309
51.83.246.184	287

Top-15 Countries Sending COVID Spam

US	6994
IN	4289
CN	2249
FR	2172
--	1771
DE	1307
RU	1100
IT	790
RO	703
JP	691

COVID-19 Email Spam Statistics (Continued)

Top Subjects Containing exe Files

vaccination covid planning presence médecins du 25 janvier au 20 fevrier	1

Top-15 Subjects Containing doc/xlsx Files

BHP – obowiązki pracodawcy i pracownika w dobie Covid 19	7
REVISION: Delivery of Healthcare Services During a Declaration of Public Health Emergency SARS-CoV-2 (COVID-19)	5
2021 Tax Season Update, COVID Update, Staff/Client Protocols, Organizer	3
COVID Vaccine Appointment	2
New vinyl like gloves and Aseptopol (covid efficacy sanitiser)	1
COVID Letter	1
Richiesta disponibilità per ENEL + questionario covid	1
RE: LISTADO ACTUAL PERSONAL PENDIENTE DE VACUNA COVID	1
Cas COVID	1
Xpart Express SARS COVID-19 Test Report.Natore	1

COVID-19 Host, Domain, and Mobile App Tracking

RiskIQ gathers data relating to newly-observed hosts and domains containing COVID-19, COVID19, or Coronavirus in the host or domain name, and mobile apps containing COVID-19, COVID19, or Coronavirus in the title or description. A summary of data collected is contained in this section.

Domain Stats

Domains: 140,199
Domains with Potential Mail Servers: 2,558
Email-Capable Domains and Hosts: 53,173
Live Hosts and Domains Not Parked: 45,784

Mobile Apps

Apps in Official Stores: 506

by Store

Apple	249
Google	240
WindowsPhone	16
Amazon	1

Apps in Secondary/Hybrid/Affiliate Stores: 2,042

by Store Type:

Hybrid	1050
Secondary	928
Affiliate	64

Blacklisted Mobile Apps: 28

by Store Type:

Secondary	25
Official	2
Hybrid	1